Available online at www.sciencedirect.com

SciVerse ScienceDirect

Physics Procedia 33 (2012) 1208 – 1211

Physics Procedia

2012 International Conference on Medical Physics and Biomedical Engineering

The Comparative Analysis of Main Access Control Technologies

Su Zhang, Li Niu, Jing Chen

Dept. of Computer Engineering, Suzhou Vocational University,Suzhou Jiangsu 215104, China
E-mail: zsu@jssvc.edu.cn

Abstract

Effective access control security design is an important precondition for the stable running of an information system. So it's necessary to establish a well-designed security mechanism to ensure the security of the system. This paper analysis and compares the main access control theories.

Keywords: Access Control; Role-based Access Control; NIST RBAC proposed standard; Mandatory Access Control; Discretionary Access Control

1.Introduction

Access control technology rising at the last century seventies, it was proposed to management the access of shared data in large hosts to ensure only the authorized user can access certain data. With the development of the computer technologies, especially with the development of web applications, the theories and methods of access control are rapidly applied in various fields of information systems. Access control means methods to explicitly permit or limit the access ability and scope. Access control are used to limit the access of key resources and to prevent the attacks of illegal users and the damages the legal users made by careless operations. In brief, the problem the access control solved is "When and where, who can operate what resources". The main access control technologies include DAC (Discretionary Access Control), MAC (Mandatory Access Control) and RBAC (Role-based Access Control).

 doi:10.1016/j.phpro.2012.05.200

2.Discretionary Access Control

DAC occurs with the development of time-sharing systems. The basic principles include: the subjects of system (users or user processes) can authorize the access privilege of objects to other subjects totally or partially. The realizing methods are usually to establish a system access control matrix, the rows of the matrix corresponding to the subjects of system, and the columns of the system corresponding to the objects of the system, the elements of the matrix corresponding to the access privileges of the subjects to the objects.

Although DAC has been implemented in systems such as UNIX, there is one deadly weakness that the access authorizations are transferable. Once the access authorizations are transferred, the management of access control will be very difficult and will lead to serious security problems. On the other hand, DAC doesn't protect the copies of the objects, so although a user can't access the object, perhaps it can access the copy of the object. That adds the management difficulty. And in large systems, the number of objects is huge, whatever kind of DAC be adopted, the following system cost is enormous and the work efficiency can't meet the need of large system especially big network applications.

3.Mandatory Access Control

MAC technology is proposed to meet the data protect requirements of secret information and the attacks of Trojan horse virus. MAC provides unavoidable access control to prevent directly or indirectly illegal intrusion. In the system, a stable security attribute will be assigned to the object also to the subject; the security attribute decides whether a subject can accesses an object. The security attributes are assigned by Security Officer, the user and the user process can't change their own security attributes.

The basic principle is acyclic information flow based on grid. Each subject in system will be assigned a security certificate, and each object will be assigned a security level. There are two key rules: can't read upper data and can't write lower data. That means data can only flow from low security level to high security level. Any actions break the rules will be forbidden. At first, MAC are mostly used in military affairs and usually be used together with DAC, subjects can access objects only when the subject pass through the check of DAC and MAC. MAC provides higher strict access control so as to prevent Trojan horse virus to steal protected data. At the same time, MAC can prevent the unconscious leakage of secret. But because in MAC, strict access controlling is inevitable, that will reduce system's flexibility.

4.Role-based Access Control

Using RBAC technology, users are associated with resources by roles, users don't know how many resources can be used, users only knows how many roles he belong to, and once the user belong to some role, the user can operate all the resources the role owned.

The basic theory of RBAC is to assign privileges of resources to roles, at the same time, users also be assigned to roles, users get privileges through the roles. The main advantage of RBAC is to simplify the complexity of authorization, and more secure and easier operate than DAC and MAC, that's why RBAC gets more support.

But the concepts of rule and privilege are very abstract, they are widely used and meaningful, on this account, roles and privileges must be specified in given environment. So up to now RBAC is still an abstract theory model, the implement of RBAC still very complex and needs intensive study.

5.NIST RBAC Proposed Standard

NIST RBAC proposed standard provide four RBAC components: Core RBAC, Hierarchical RBAC, Static Separation of Duties and Dynamic Separation of Duties.

The main concepts in NIST RBAC proposed standard are as follows.

- Subject

Subject is the object which can operate other objects, usually means system users or system processes.

- User

User means the people who want to use the system. Each user has a user-identification (UID), system do the authentication by UID.

- Object

Object means the thing be operated by other things. Usually Object means system resources, such as files and database data and so on. An entity can be subject sometimes and be object at other times, which rely on the role the entity playing in the action, being performer of the action or being the accepter of the action.

- Role

The concept of Role has rich meaning, the introducing of Role into Access Control, expanding the content of Access Control and making the implement of Access Control more flexible. Simply, Role can be understood as the position of a person in an enterprise. The Role means the union of the operation the person on the position can use. And because in RBAC, Users are assigned to Roles, the same time Permissions also assigned to Roles, so Role can also be understood as the union of users and permissions.

- Permission

Permission is an abstract concept, which means the permission of the operating on some subject. The abstract of Permission mainly means the variety of operations. For example, in file systems, operating means the reading, writing and the executing of some file. And for database management systems, operating means the inserting, deleting and updating some data.

- User-to-Role Assignment

User-to-Role Assignment means the action of assign users to roles. A user can be assigned to several roles and a role can be assigned to several users. It's many-to-many relationship.

- Permission-to-Role Assignment

Permission-to-Role Assignment means the action of assign permissions to roles. It's many-to-many relationship. Thus, users are combined with permissions through roles. And a user has the summation of the permissions of all the roles he assigned to owning.

- Session

Session means the mapping of a user and roles in some environment, which means the set of roles be activated to accomplish some tasks. The summation of the permissions of the roles being activated is the set of the permissions the user can use in that situation.

- Role Hierarchical

Role Hierarchical is an expansion of Core RBAC. Role Hierarchical is a partial ordering relationship in the strict sense. The higher roles inherit the permissions of lower roles and the lower roles gain the users of higher roles. And according to whether there being restrictions in the partial ordering relationship, there are two situations.

All-purpose Hierarchical RBAC support any kinds of partial ordering relationship, and support the various hierarchical, a role can have many sub-roles, and have many parent-roles at the same time.

Restricted Hierarchical RBAC adds restrictions in partial ordering relationship, so that to make the structure of hierarchical more simple, for example to be a tree or an inverse tree.

Roles are specified to different hierarchical is a big advantage of RBAC. Usually, role hierarchical can be structured according to the inner structure of a corporation.

- Static Separation of Duties (SSD)

In the Hierarchical RBAC, user can be assigned to two conflicting roles, which will lead to conflict permission assignment. Static Separation of Duties means adding restrictions in the User-to-Role Assignment to avoid the conflicts. So after a user being assigned to a role, the user will be forbidden to be assigned to other conflict roles. Besides the roles separation of duties, there also has permissions separation of duties.

- Dynamic Separation of Duties

Similar to SSD, Dynamic Separation of Duties also provides restricts of the permissions of users. But different from SSD, DSD activate restrictions in sessions. In SSD, conflict roles can't be assigned to the same user, but in DSD, conflict roles can be assigned to the same user, but they can't be activated in one session. That ensures a user won't have the conflict permissions in one session.

6.Access Control Methods Comparison

DAC directly combines users and resources and operations, using lists and matrixes recording the resources and the operations a user can execute. MAC always be used in military systems, which won't combines users and resources, but assign security level to each user and resource. And user can only operate the resources which has lower security level. RBAC combines users and permissions through roles. A user don't know how many resources he can operate, he only knows how many roles he belongs to, once he belongs to some role, he can operate the resources be assigned to the role.

With the development of the distributed systems, RBAC models are more practical and flexible. Recently the research in RBAC mainly concerns the research of theory models and the research of the implement of models. The research of models means the modifying and developing of models, to rich the content of models. And the research of implement means according to the given situation, to extend and adjust the model to meet the requirements of the implement system.

7.Conclusions

A system running, security ability should be carefully designed, that's the way to ensure the stable running of the system. This paper mainly analysis and compares all kinds of access control theories, to prepare for the next phase of study.

References

[1] Ravi S. Sandhu. Access Control. The neglected frontier[Z]. ACISP/1996.

[2] David F. Ferraiolo, Ravi S. Sandhu, Serban Gavrila, D. Richard Kuhn and Ramaswamy Chandr-amouli. Proposed NIST standard for role-base access control[J]. ACM Transactions on Information and Systems Security, Aug 2001, (3):224~274.

[3] Zhang Su. Design and Implementation of Access Control Model for Web Application Integration [D]. Suzhou: Soochow university, 2005.

[4] Zhang Su, Li Pei-feng, Yang Ji-wen. Design and implementation of unified access control platform for web application integration [J]. Computer Engineering and Design, 2006(08):1369~1381